EUROPEAN PUBLIC PROSECUTOR'S OFFICE

EPPO

EUROPOL

Working Arrangement establishing cooperative relations between the European Public Prosecutor's Office and the European Union Agency for Law Enforcement Cooperation

The European Public Prosecutor's Office
(hereafter referred to as "EPPO")

and

the European Union Agency for Law Enforcement Cooperation
(hereafter referred to as "Europol")

– together referred to as "The Parties" –,

Considering the objective the Union has set itself of establishing an area of freedom, security and justice, and the respective roles the Parties play towards achieving this objective in accordance with their mandates,

Considering Articles 22, 23 and 102 as well as recitals 69 and 100 of the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the EPPO (hereafter referred to as "EPPO Regulation"), as well as that the College of the EPPO has on 25 November 2020 approved the present Working Arrangement,

Considering Articles 3, 4(1)(j), 23 and 24 of the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation as amended (hereafter referred to as "Europol Regulation") as well as that the Europol Management Board has on 10 December 2020 approved the present Working Arrangement,

Have agreed as follows:

Chapter I – Purpose and Scope

Article 1
Purpose

The purpose of this Working Arrangement (hereafter referred to as "Arrangement") is to establish cooperative relations between the EPPO and Europol within the existing limits of the respective legal frameworks and mandates of the Parties, in particular through the exchange of information between the Parties.

Article 2
Definitions

For the purpose of this Arrangement:

a) "personal data" means any information relating to an identified or identifiable natural person, an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

b) "information" means personal and non-personal data.

Article 3
Areas of crime

The cooperation as established in this Arrangement shall relate to the relevant areas of crime in respect of which both Parties are competent, including specifically criminal offences affecting the financial interests of the European Union which are provided for in Directive (EU) 2017/1371, as implemented by national law and in the EPPO Regulation.

Article 4
Areas of cooperation

The cooperation may, additional to the exchange of information under the conditions laid down in this Arrangement, in accordance with the tasks of the Parties as outlined in their respective legal frameworks, in particular include the exchange of specialist knowledge,

general situation reports, information on criminal investigation procedures, information on crime prevention methods, the participation in training activities as well as providing advice and support, including through analysis, in individual criminal investigations.

Chapter II – Mode of cooperation

Article 5
Point of Contact

Each Party shall designate a single point of contact through which all exchange of operational information under this Arrangement is undertaken.

Article 6
Consultations and closer cooperation

The Parties agree that regular exchanges, as appropriate, are integral to further the cooperation and enhance as well as monitor the development of the provisions of this Arrangement. Specifically:

- High level meetings between the EPPO and Europol shall take place regularly to discuss issues relating to this Arrangement and the cooperation in general.

- The EPPO and Europol shall consult each other regularly on policy issues and matters of common interest for the purpose of realising their objectives and coordinating their respective activities.

- Where relevant, a representative of the EPPO may attend the meetings of the Heads of Europol National Units as observer.

Article 7
Liaison officers or experts

The Parties may agree to the secondment of liaison officer(s) or expert(s). Their tasks, rights and obligations, their number, and the costs involved shall be governed by a separate instrument agreed between the Parties.

Chapter III – Information exchange

Article 8
General provisions

1. Exchange of information between the Parties shall only take place in accordance with their respective legal framework and the provisions of this Arrangement.

2. Parties shall only supply information to each other which was collected, stored and transmitted in accordance with their respective legal framework. Europol, in line with Article 23(9) of the Europol Regulation, shall not process any information which has clearly been obtained in obvious violation of human rights.

3. Individuals shall have, in accordance with the respective legal framework of either Party, the right to access the personal data related to them transmitted on the basis of the present Arrangement, and to have such personal data checked, corrected or deleted. In cases where these rights are exercised, the transmitting Party shall be consulted before a final decision on the request is taken, including concerning possible applicable restrictions to the rights of the data subject. The final decision shall be subsequently notified to the transmitting party.

4. Requests for public access to information transmitted on the basis of the present Arrangement shall be submitted to the transmitting Party for their advice as soon as possible.

Article 9
Exchange of personal data

1. Any exchange of personal data shall be in accordance with and based upon the Parties' respective legal frameworks.

2. The Parties shall determine at the moment of transmission of the personal data or before, the purpose for which the data are transmitted, and any restriction on its use, deletion or destruction, including possible access restrictions in general or specific terms. Where the need for such restrictions becomes apparent after the supply, the transmitting Party shall inform of such restrictions at a later stage.

3. The Parties shall determine without undue delay, no later than six months after receipt, if and to what extent the personal data which have been supplied are

necessary for the purpose for which they were supplied and inform the transmitting Party thereof. The personal data shall be deleted when the data is not necessary for the purpose for which they were transmitted.

4. The Parties shall retain personal data only as long as it is necessary and proportionate for the purpose for which it was transmitted. The need for continued storage shall be reviewed no later than three years after the transmission. During the review, each Party may decide on the continued storage of data until the following review which shall take place after another period of three years if that is still necessary for the performance of its tasks. If no decision is taken on the continued storage of data, those data shall be deleted automatically.

5. Where a Party has reason to believe that personal data previously transmitted by it is incorrect, inaccurate, no longer up to date or should not have been transmitted, it shall inform the other Party which shall correct or delete the personal data and provide notification thereof.

6. Where a Party has reason to believe that personal data previously received by it is incorrect, inaccurate, no longer up to date or should not have been transmitted, it shall inform the other Party which shall provide its position on the matter.

7. In line with the Parties' respective legal frameworks, personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data or data concerning a person's health or sex life shall not be transmitted between the Parties unless such transmission is strictly necessary and proportionate.

Article 10
Use of the information

1. Information if transmitted with a purpose, notwithstanding the obligation to do so as per Article 9(2), may be used only for the purpose for which it was transmitted and any restriction on its use, deletion or destruction, including possible access restrictions in general or specific terms, shall be respected by the Parties.

2. Use of information for a different purpose than the purpose for which the information was transmitted shall be authorised by the transmitting Party.

Article 11
Onward transmission of the information received

Any onward transmission, including to Union bodies, Member States, third countries and international organisations, shall receive the prior explicit authorisation by the transmitting Party, in specific or in general terms. Such consent may only be given when allowed under the applicable legal framework of the transmitting Party.

Article 12
Assessment of the source and of the information

1. When information is supplied by the Parties on the basis of this Arrangement, the reliability of the source of the information shall be assessed as far as possible on the basis of the following criteria:

   (A) Where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances;

   (B) Source from whom information received has in most instances proved to be reliable;

   (C) Source from whom information received has in most instances proved to be unreliable;

   (X) The reliability of the source cannot be assessed.

2. When information is supplied by the Parties on the basis of this Arrangement, the accuracy of the information shall be assessed as far as possible on the basis of the following criteria:

   (1) Information whose accuracy is not in doubt;

   (2) Information known personally to the source but not known personally to the official passing it on;

   (3) Information not known personally to the source but corroborated by other information already recorded;

   (4) Information which is not known personally to the source and cannot be corroborated.

3. If either of the Parties, on the basis of information already in its possession, comes to the conclusion that the assessment of information supplied by the other Party needs correction, it shall inform the other Party and attempt to agree on an

amendment to the assessment. Neither of the Parties shall change the assessment of information received without such agreement.

4. If a Party receives information without an assessment, it shall attempt as far as possible and in agreement with the transmitting Party to assess the reliability of the source or the information on the basis of information already in its possession.

5. The Parties may agree in general terms on the assessment of specified types of information and specified sources, which shall be laid down in a Memorandum of Understanding between the EPPO and Europol. If information has been supplied on the basis of such general agreements, this shall be noted with the information.

6. If no reliable assessment can be made, or no agreement in general terms exists, the information shall be evaluated as at paragraph 1 ("X") and paragraph 2 ("4") above.

Article 13
Security of processing of personal data

1. The Parties shall ensure that the personal data exchanged or received is protected through technical and organisational measures. Such measures shall only be necessary where the effort they involve is proportionate to the objective they are designed to achieve in terms of protection, and will be designed to:

   a) deny unauthorised persons' access to data processing equipment used for processing personal data (equipment access control),

   b) prevent the unauthorised reading, copying, modification or removal of personal data media (data media control),

   c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (storage control),

   d) prevent the use of automated data-processing systems by unauthorised persons using data-communication equipment (user control),

   e) ensure that persons authorised to use an automated data-processing system have access only to the personal data covered by their access authorisation (data access control),

   f) ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted using data communication equipment (communication control),

g) ensure that it is possible to verify and establish what personal data have been accessed by which member of personnel and at what time (access log),

h) ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the personal data were input (input control),

i) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control),

j) ensure that installed systems may, in the event of interruption, be restored immediately (recovery),

k) ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability) and that stored personal data cannot be corrupted by system malfunctions (integrity).

2. The Parties shall handle security incidents, including personal data breaches, in accordance with their applicable legal frameworks and internal procedures. The Parties shall immediately notify each other in the event of any personal data breach related to personal data exchanged under this Arrangement and of any measures taken to address the personal data breach and to mitigate the risk to the rights and freedoms of natural persons.

Chapter IV – Security of information

Article 14
Protection of information

Each Party shall:

1. protect information subject to this Arrangement, regardless of its form, until it has reached its end of life and is securely destroyed. This obligation shall not apply to information which is expressly marked or clearly recognisable as public information,

2. ensure that it has a security organisation, policies and measures in place to comply with the requirements set out in this Arrangement,

3. manage information security risks for all systems processing information exchanged under this Arrangement and assess these risks on a regular basis and whenever there is a significant change to any of the risk components,

4. ensure that all persons handling information exchanged under this Arrangement are subject to a security screening in accordance with the legal framework of the receiving Party,

5. ensure that access to information is limited to authorised persons who need to have access to it in order to perform their official duties,

6. ensure that all persons handling information exchanged under this Arrangement are appropriately trained and familiar with the relevant security rules, policies and procedures,

7. ensure that all staff handling information exchanged under this Arrangement are made aware of their obligation to protect the information and acknowledge the obligation in writing,

8. ensure that the premises where information exchanged under this Arrangement is stored or handled have an appropriate level of physical security in accordance with the legal framework of the receiving Party,

9. ensure that it has a framework in place for reporting, managing and resolving security incidents and breaches.

Article 15

Arrangement on the exchange and protection of classified information

1. The security procedures for exchanging and protecting classified information exchanged between the Parties shall be set out in an arrangement on the exchange and protection of classified information agreed between the Parties.

2. Without prejudice to any other provisions of the respective legal frameworks permitting exceptional transfers of classified information, exchange of classified information is conditional upon the conclusion of the arrangement on the exchange and protection of classified information.

Chapter V – Disputes and liability

Article 16

Liability

1. The Parties shall be liable, in accordance with their respective legal frameworks, for any damage caused to an individual as a result of legal or factual errors in

information exchanged. In order to avoid its liability under their respective legal frameworks vis-à-vis an injured party, neither Party may plead that the other had transmitted inaccurate information.

2. If these legal or factual errors occurred as a result of information erroneously communicated or of failure on the part of the other Party to comply with their obligations, they shall be bound to repay, on request, any amounts paid as compensation under paragraph 1 above, unless the information was used by the other Party in breach of this Arrangement.

3. The Parties shall not require each other to pay for punitive or non-compensatory damages under paragraphs 1 and 2 above.

Article 17
Settlement of disputes

1. All disputes which may emerge in connection with the interpretation or application of the present Arrangement shall be settled by means of consultations and negotiations between representatives of the Parties.

2. In the event of serious failings of either Party to comply with the provisions of this Arrangement, or is a Party of the view that such a failing may occur in the near future, either Party may suspend the application of this Arrangement temporarily, pending the application of paragraph 1. Obligations inherent upon the Parties under the Arrangement will nonetheless remain in force.

Chapter VI – Final provisions

Article 18
Secure communication line

1. The establishment, implementation and operation of a secure communication line for the purpose of exchange of information between the EPPO and Europol shall be agreed upon between the Parties in a Memorandum of Understanding.

2. Without prejudice to Article 16, a Party shall be liable for damage caused to the other Party as a result of wrongful actions relating to the establishment, implementation or operation of the secure communication line.

3. Any dispute between the Parties concerning the interpretation or application of provisions relating to the establishment, implementation or operation of the secure communication line shall be settled in accordance with Article 17.

Article 19
Expenses

The Parties shall bear their own expenses which arise in the course of implementation of the present Arrangement, unless otherwise stipulated in this Arrangement.

Article 20
Amendments and supplements

1. This Arrangement may be amended in writing at any time by mutual consent between the Parties. Any amendment must receive the appropriate approval in line with the Parties' respective legal frameworks.

2. Two years after the entry into force of the Arrangement, any Party may, on the basis of experience gathered during the practical implementation thereof, suggest to the other Party to amend the Arrangement in line with paragraph 1.

Article 21
Entry into force

This Arrangement shall enter into force on the day following the date of the last signature.

Article 22
Termination of the Arrangement

1. This Arrangement may be terminated in writing by either Party with three months' notice.

2. In case of termination, the Parties shall reach agreement on the continued use and storage of the information that has already been communicated between them.

3. Without prejudice to paragraph 1, the legal effects of this Arrangement shall remain in force.

Done in duplicate in the English language.

For the **European Public Prosecutor's Office**

Laura Kövesi
European Chief Prosecutor

Done at Luxembourg
on 18 / 01 / 2021

For **Europol**

Catherine De Bolle
Executive Director

Done at The Hague
on 11 / 01 / 2021.